

Docket No. AUS9-2000-0401-US1

CLAIMS:

What is claimed is:

1. A method for filtering incoming data from an external computer network, comprising:
 - scanning the content of incoming data for pre-selected keyword(s);
 - blocking the incoming data if the content contains pre-selected keywords; and
 - adding the address of a blocked site to a filtering table.
2. The method according to claim 1, wherein the step scanning the content of incoming data includes scanning the text fields within the body of the transmission.
3. The method according to claim 1, wherein the incoming data is allowed to pass per standard service rules if the content does not contain pre-selected keyword(s).
4. The method according to claim 1, further comprising a filtering table of "known-safe" sites that can be passed per standard service rules without having to be scanned for pre-selected keywords.
5. The method according to claim 1, wherein the step adding the address of a blocked site to a filtering table, includes adding the site to a "known-block" table so that the site will be blocked in the future without having its contents scanned for pre-selected keywords.

6. The method according to claim 1, wherein the addition of a site to the filtering table is implemented using a strong text parsing language.

7. The method according to claim 1, wherein the instance of the filter is periodically refreshed through a timed job on a Windows NT platform, a cron job on a UNIX platform, to enact the updated filtering tables.

8. A computer program product in a computer readable medium for use in a data processing system for filtering incoming data from an external computer network, the computer program product comprising:

instructions for scanning the content of incoming data for pre-selected keyword(s);

instructions for blocking the incoming data if the content contains pre-selected keywords; and

instructions for adding the address of a blocked site to a filtering table.

9. The computer program product according to claim 8, wherein the instructions for scanning the content of incoming data include instructions for scanning the text fields within the body of the transmission.

10. The computer program product according to claim 8, further comprising instructions for allowing incoming data to pass per standard service rules if the content does not contain pre-selected keyword(s).

11. The computer program product according to claim 8, further comprising instructions for creating a filtering table of "known-safe" sites that can be passed per

002100-101200

standard service rules without having to be scanned for pre-selected keywords.

12. The computer program product according to claim 8, wherein the instructions for adding the address of a blocked site to a filtering table, includes instructions for adding the site to a "known-block" table so that the site will be blocked in the future without having its contents scanned for pre-selected keywords.

13. The computer program product according to claim 8, wherein the instructions for addition of a site to the filtering table are implemented in a strong text parsing language.

14. The computer program product according to claim 8, wherein the instance of the filter is periodically refreshed through a timed job on a Windows NT platform, a cron job on a UNIX platform, to enact the updated filtering tables.

15. A system for filtering incoming data from an external computer network, the system comprising:

means for scanning the content of incoming data for pre-selected keyword(s);

means for blocking the incoming data if the content contains pre-selected keywords; and

means for adding the address of a blocked site to a filtering table.

002101-00128950